UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/615,967	07/14/2000	Michael P. Lyle	RECOP001	6546

21912 7590 01/27/2005

VAN PELT & YI LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
HENEGHAN, MATTHEW E	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 01/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/615,967	LYLE ET AL.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 August 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17 and 30-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17 and 30-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 August 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. In response to the previous office action, Applicant has amended claims 1-3, 12, 16, 30, and 32 and added claim 33.

2. Claims 1-17 and 30-33 have been examined.

Response to Amendment

3. The amendment filed 9 August 2004 is objected to under 35 U.S.C. 132 because it introduces new matter into the disclosure. 35 U.S.C. 132 states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: Claims 1, 30, and 32 each include a limitation "wherein the quantity and substance of the generated content are such that the deception environment would present to an intruder a credible version of a system such as the intruder would expect to see upon gaining unauthorized access to the computer." This limitation is not supported by the original specification.

Applicant is required to cancel the new matter in the reply to this Office Action.

Drawings

4. The drawings were received on 9 August 2004. These drawings are acceptable.

Double Patenting

5. In view of Applicant's amendment, the previous double patenting rejections have been withdrawn.

Claim Rejections - 35 USC § 112

6. In view of Applicant's amendment, all previous rejections under 35 U.S.C. 112 are withdrawn.

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 1-17 and 30-33 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The claims are also rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in

such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Claims 1, 30, and 32 each include a limitation "wherein the quantity and substance of the generated content are such that the deception environment would present to an intruder a credible version of a system such as the intruder would expect to see upon gaining unauthorized access to the computer. This limitation is not supported by the original specification; moreover, no standard is disclosed by which one skilled in the art could ascertain what would constitute a "credible version of a system."

For purposes of the prior art search, this limitation is being ignored.

Claims 2-18, 31, and 33 depend from rejected claims 1 and 30, and include all the limitations of those claim, thereby rendering those dependent claims as not complying with 35 U.S.C. 112, first paragraph.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claim 33 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "cage" in claim 33 is a term which renders the claim indefinite. The term "cage" is not defined by the claim, the specification does not provide a standard for ascertaining what constitutes a "cage." One of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

For purposes of the prior art search, it is being presumed that a cage comprises a functionality coherent subset of a computer system.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 1, 2, 6, 12, 14, 30, 32, and 33 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 4,719,566 to Kelley.

Note: Kelley was cited in a previous Office Action.

As per claims 1, 30, 32, and 33, Kelley discloses a system that is associated with a network ("uses VTAM/SNA," which is a network protocol, see column 3, lines 25-27); gives an example of a trap node called LAXPRESS having an operating system and generated content, such as a logo (see column 4, lines 28-37); and routes a user based on a non-user-specific policy, such as excessive invalid logon attempts (see column 3, lines 49-55).

As per claims 2 and 6, the intruder is bound to the false system, where monitoring takes place (see column 3, lines 49-55).

As per claim 12, a network address translation (to SECSYS ID) is performed for users making invalid requests (see column 6, lines 15-20).

As per claim 14, a LOGISOFF message is sent to a list of Ids when the intruder logs off (see column 5, lines 23-28).

10. Claims 1-4 and 30-32 are rejected under 35 U.S.C. 102(a) as being anticipated by Spitzner, "To Build a Honeypot," 1999.

As per claim 1, 30, and 32, Spitzner discloses a honeypot that contains automatically generated a system inherently having content (a mirror of a production system), using a fully functional operating system such as Linux (see "Where to Begin?" pp 1-2); and has a policy that all users accessing the honeypot gets routed to the deception environment (see "The Plan," second bulletpoint, p.2).

As per claim 2, the system creates logs to track users (see "Tracking Their Moves," p.2).

As per claim 3, the real configuration file is placed in an area inaccessible to the user, on a syslog server (see p.3, first paragraph).

As per claim 4, a sniffer is used to store the user's packets (see p.3, third paragraph).

As per claim 31, the system of Spitzner comprises a firewall (see "The Plan," second bulletpoint, p.2).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 5 and 7-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spitzner, "To Build a Honeypot," 1999 as applied to claim 1 above, and further in view of U.S. Patent No. 5,925,126 to Hsieh.

Spitzner does not disclose the logging of all file access attempts.

Hsieh discloses a security system wherein file accesses are logged and file access requests are screened and the operating system is instructed as to whether to grant the request or stop the process (see column 5, lines 46-67), and suggests that this helps protect a computer system from unauthorized access by a user (see column 4, lines 15-19).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system disclosed by Spitzner by logging file accesses and instructing as to whether to grant the request or stop the process, as disclosed by Hsieh, as that this helps protect a computer system from unauthorized access by a user.

Regarding claims 10 and 11, content could be changed any of a number of times after it is initially constructed. It is noted, however, that the art references cited above

only sets up the content at the beginning, and have no mechanism for further modifying the content after the intruder has arrived. Cheswick, cited in the previous office action, disclosed such a modifying of content, but this was not being done automatically.

12. Claims 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 4,719,566 to Kelley as applied to claim 12 above, and further in view of U.S. Patent No. 5,925,126 to Hsieh.

Kelley does not disclose the ingress being used by uses that are to be rerouted.

Hsieh also discloses system call interception in order to directly handle users getting access by means such as telnet, and suggests that protecting against the system console terminal alone is not sufficient because alternative paths exist (see column 5, lines 28-45 and column 6, column 66 to column 7, line 14).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system disclosed by Kelley by directly handling users getting access by means such as telnet, as disclosed by Hsieh, as protecting against the system console terminal alone is not sufficient because alternative paths exist.

Allowable Subject Matter

13. Claims 15-17 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

14. The following is a statement of reasons for the indication of allowable subject matter:

Claim 15 would be allowable because none of the art cited makes an automatic determination as to whether or not to retain the intruder's changes. All of the art either deletes all changes or requires operator intervention.

The additional limitation of claim 16 is disclosed by Spitzner, but claim 16 nonetheless would be allowable based upon its dependence on claim 15.

Claim 17 would be allowable based upon its dependence on claim 15.

Response to Arguments

15. Applicant's arguments filed 9 August 2004 regarding the status of the two priority applications have been fully considered but they are not persuasive. In order for an application to claim benefit from a priority application, at least one claim must be enabled in compliance with 35 U.S.C. 112, first paragraph; in order for a disclosure to be considered to be enabling, the written description must be sufficient for one skilled in the art to make and use the invention. Though the priority documents clearly are

sufficient for one to use Applicant's invention, neither is described in sufficient detail to allow one to *make* the invention. See MPEP 201.11(A) and 2164.

16. Applicant's arguments, see Remarks, filed 9 August 2004, with respect to the rejection(s)of claim(s) 1-17 and 29-32 under 35 U.S.C. 102 and 103 have been fully considered and are persuasive in view of Applicant's amendments. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection for some of the claims are made in view of the art cited above.

Conclusion

17. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (571) 272-3834. The examiner can normally be reached on Monday, Tuesday, Thursday, and Friday from 8:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached at (571) 272-3838.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(703) 872-9306

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MEH

January 21, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100